Panel on Security of the Internet Infrastructure

Russ Mundy, Chair mundy@tis.com
Principal Networking Scientist
Trusted Information Systems, Inc., Glenwood, Maryland, 21738, USA

Abstract

This panel will provide information on current and emerging improvements to security for the Internet infrastructure. Presentations will identify a number of current Internet short-comings and describe approaches to resolve these short-comings.

Panel Overview

The Internet has been developing and changing over many years. A large proportion of current Internet capabilities resulted from research projects. These research projects were often developing capabilities for the first time and, as a result, they focused on defining a capability then determining if it could be implemented at all. Security has seldom been an important consideration in developing new capabilities for the Internet. Since most research has focused on the primary function of a given capability, security aspects were generally ignored or deferred for later study.

Heterogeneity, interoperability and change have also been hallmarks of the Internet. The Internet has grown from a few diverse computers at research institutions to millions of computers that are located in most of the countries in the world. Today the Internet provides the capability for a small computer in a remote part of the world to communicate with some of the most powerful super-computers in existence.

Although the Internet Engineering Task Force (IETF) has defined a process for developing and publishing Internet standards, the IETF credo continues to be expressed by the phrase "rough consensus and running code". When this approach is further complicated by the fact that there are many different meanings to "security" in the Internet, this panel may seem like an oxymoron.

Most of the highly publicized Internet "security incidents" have primarily impacted end-user systems rather than Internet infrastructure systems. However, most of the factors that have made end-user systems vulnerable to attack also make the Internet infrastructure similarly vulnerable. For instance, having a network with switches from different manufactures operating together and managed remotely by a system from yet another manufacturer was unheard of before the Internet. However, these capabilities were developed and are now widely used in the Internet with minimal or no security.

This panel will have presentations on several aspects of security related to the Internet infrastructure. The Internet Protocol (IP) is sometimes referred to as the "glue of the Internet" since it provides the most basic component for many of the Internet's capabilities. Unfortunately, the original IP development did not include security capabilities. The panel will discuss the work that has been underway for several years to provide a standard approach for IP security capabilities.

Another infrastructure component that was developed and fielded without security capabilities is the Domain Name System (DNS). The DNS provides the capability to associate names with Internet addresses. This, in turn, permits users to describe services and locations in language they understand. In today's Internet, there is nothing to prevent one system from effectively stealing another system's name and, therefore, all of the connections and information intended for the legitimate owner of the name. The panel will provide a description and status of on-going activities to provide security for DNS.

In addition to these topics, the panel will also provide information on other areas, such as security for network management, that will provide improvements to the security of the Internet infrastructure.